BÁO CÁO THỰC HÀNH

Môn học: Hệ thống tìm kiếm, phát hiện và ngăn ngừa xâm nhập

Lab 03 – Viết rules trên Snort

GVHD: Đỗ Hoàng Hiển

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT204.O21.ANTT.2

STT	Họ và tên	MSSV	Email
1	Nguyễn Viết Dũng	21520747	21520090@gm.uit.edu.vn
2	Lưu Thị Huỳnh Như	21521242	21521112@gm.uit.edu.vn
3	Lê Đoàn Trà My	21521149	21521149@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:[1]

STT	Công việc	Kết quả tự đánh giá
1	Yêu cầu 1.1	100%
2	Yêu cầu 1.2	100%
3	Yêu cầu 1.3	100%
4	Yêu cầu 1.4	100%
5	Yêu cầu 1.5	100%

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

[1] Ghi nội dung công việc, yêu cầu trong bài Thực hành

BÁO CÁO CHI TIẾT

1. Yêu cầu 1.1: Giới hạn gói tin đến dịch vụ DNS đến máy Victim: không quá 90 gói/10s

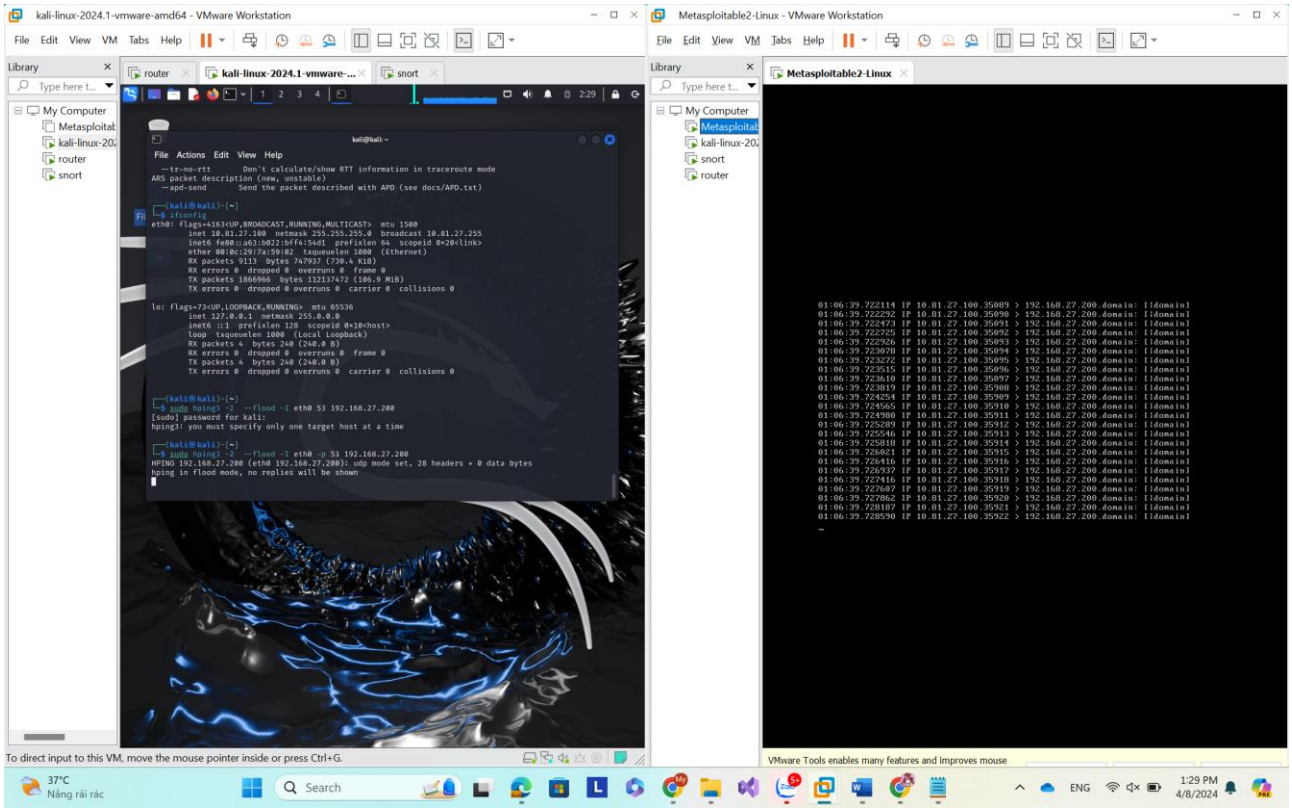
- Snort rules:

drop udp any any -> 192.168.27.200 53 (msg:"over 90 packet per 10 sec for DNS"; threshold: type limit, track by_dst, count 90, seconds 10; sid:1000001; rev:1;)

- Trước khi cài rules:

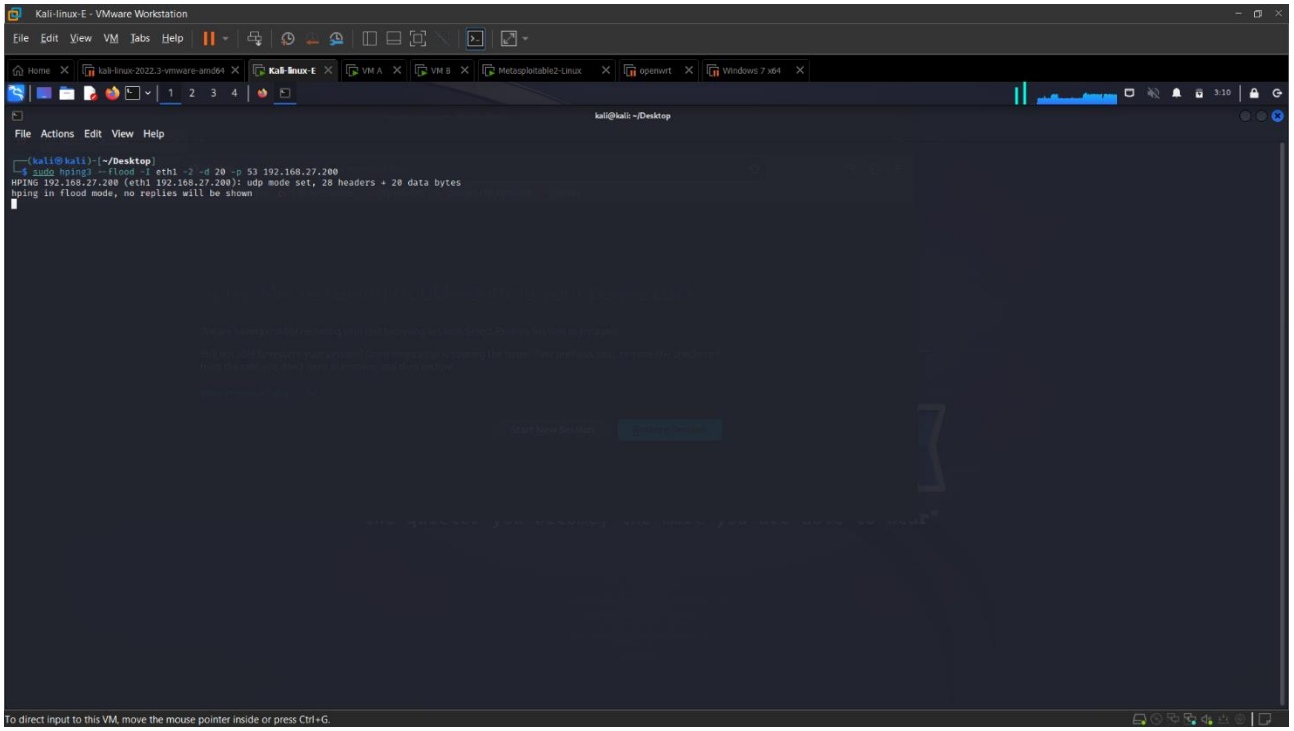
+ Phía bên attacker thực hiện flood các gói upd dns: sudo hping3 -2 --flood -I eth0 -p 53 192.168.27.200

+ Phía bên victim bật tcpdump, nhận thấy rất nhiều gói tin được truyền đến

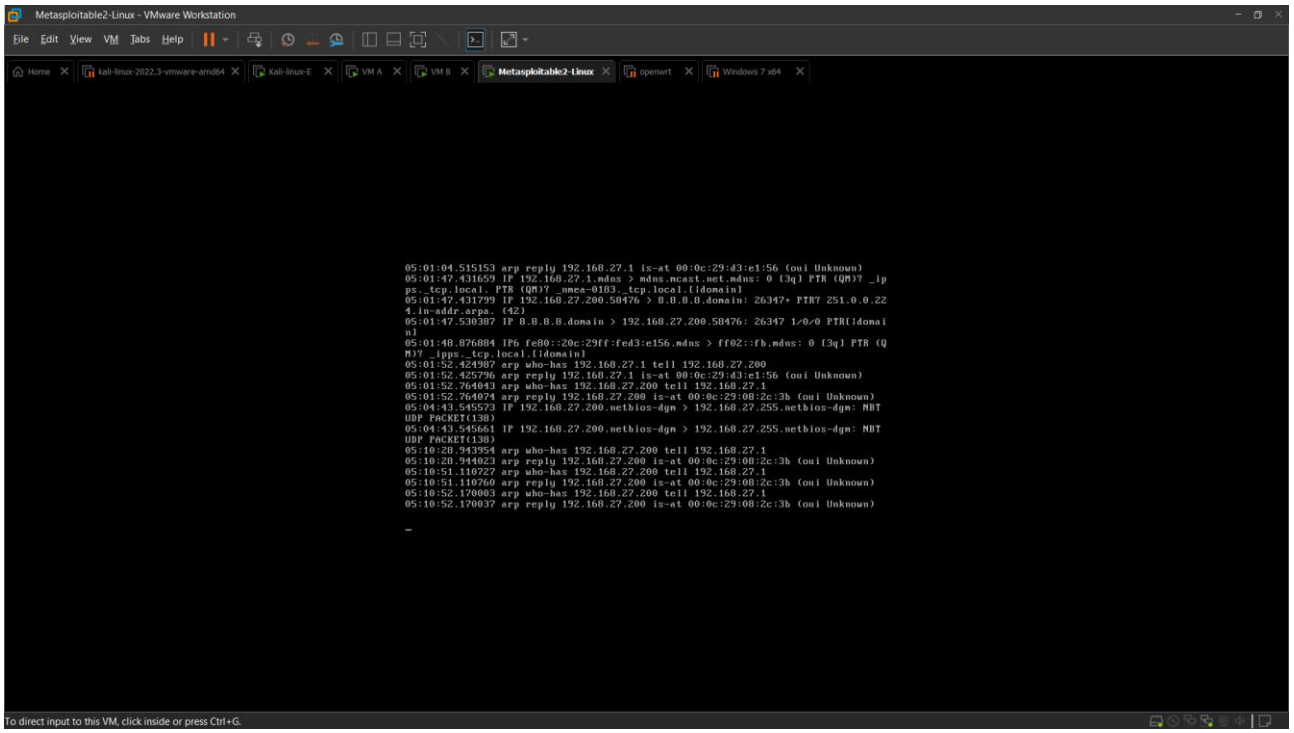


- Sau khi cài rules:

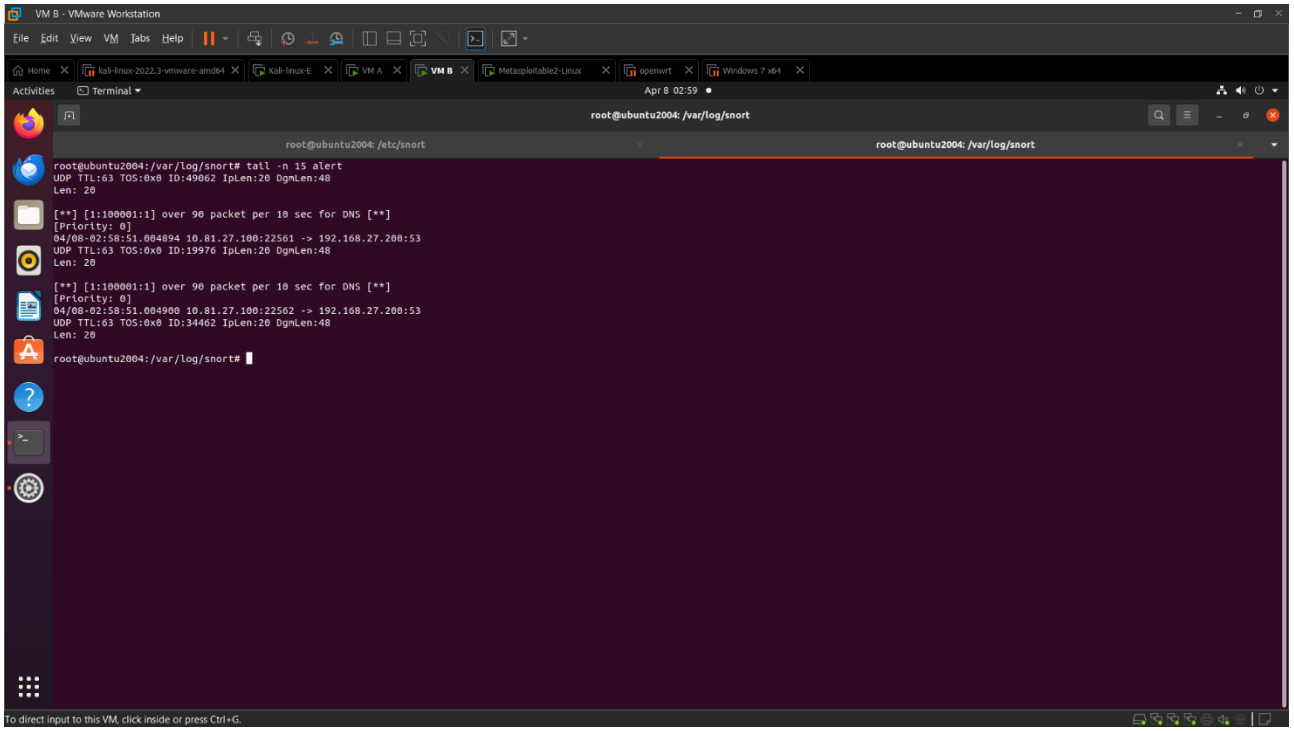
+ Phía bên attacker thực hiện flood các gói upd dns



+ Phía bên victim không hiển thị các gói truy vấn dns liên quan giữa attacker và victim



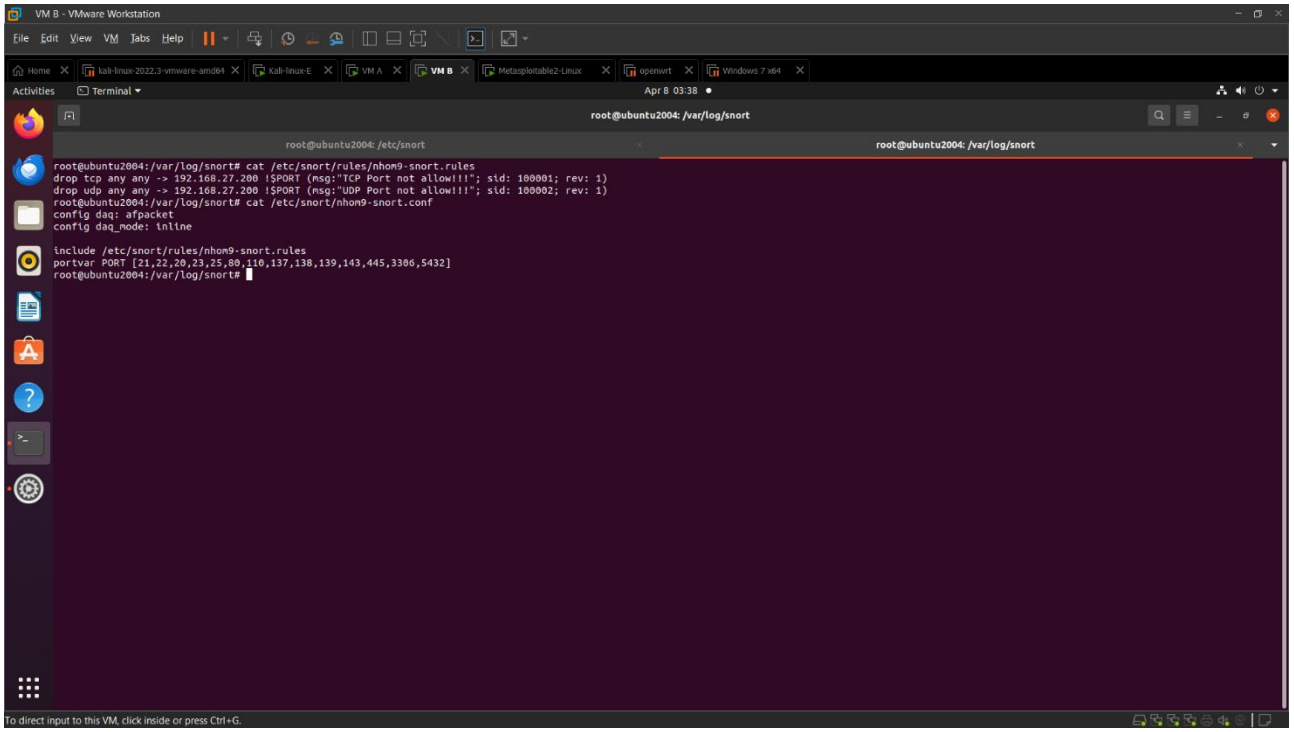
+ Trong log của snort ghi lại thông tin:



2. Yêu cầu 1.2: Chỉ cho phép truy cập đến một số dịch vụ: Telnet, FPT, SSH, Web, mail, NetBIOS, SMB, MySQL, postgresql

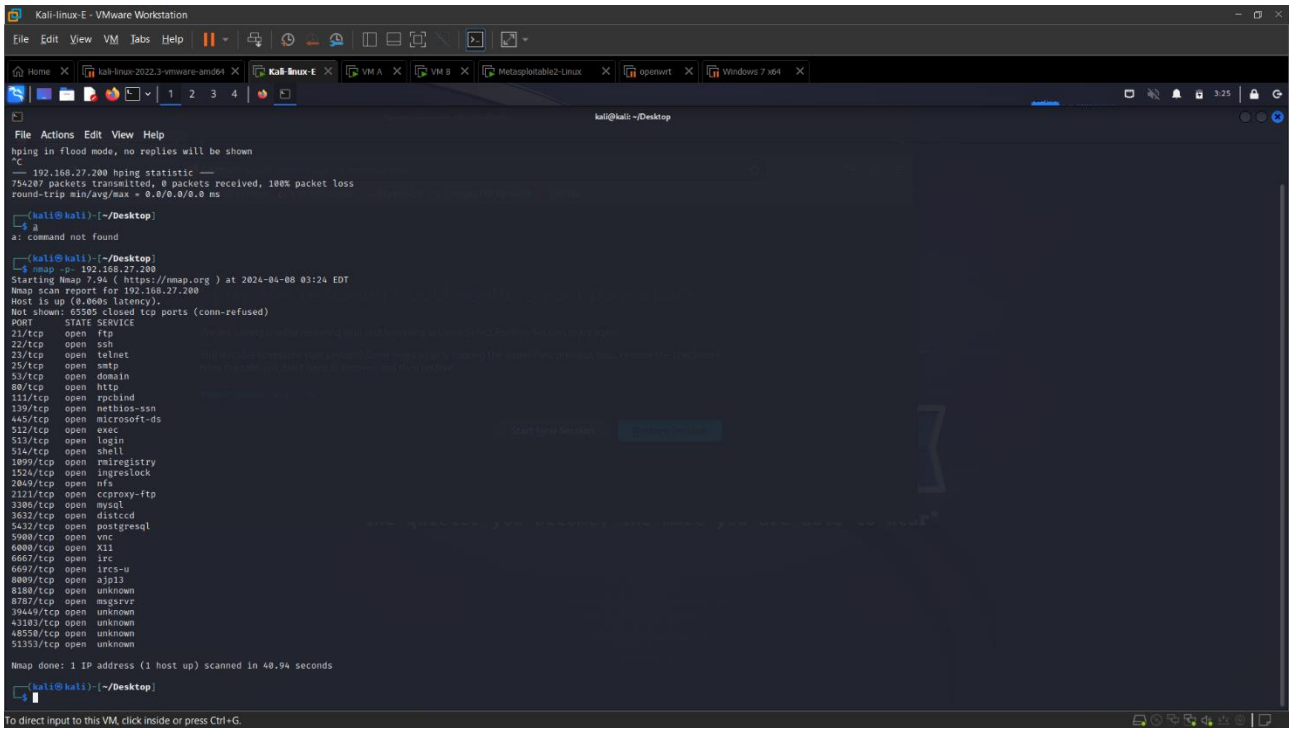
- Cho phép các máy truy cập đến các port đang mở của máy Victim. Chặn tất cả các port còn lại

- Snort rules:

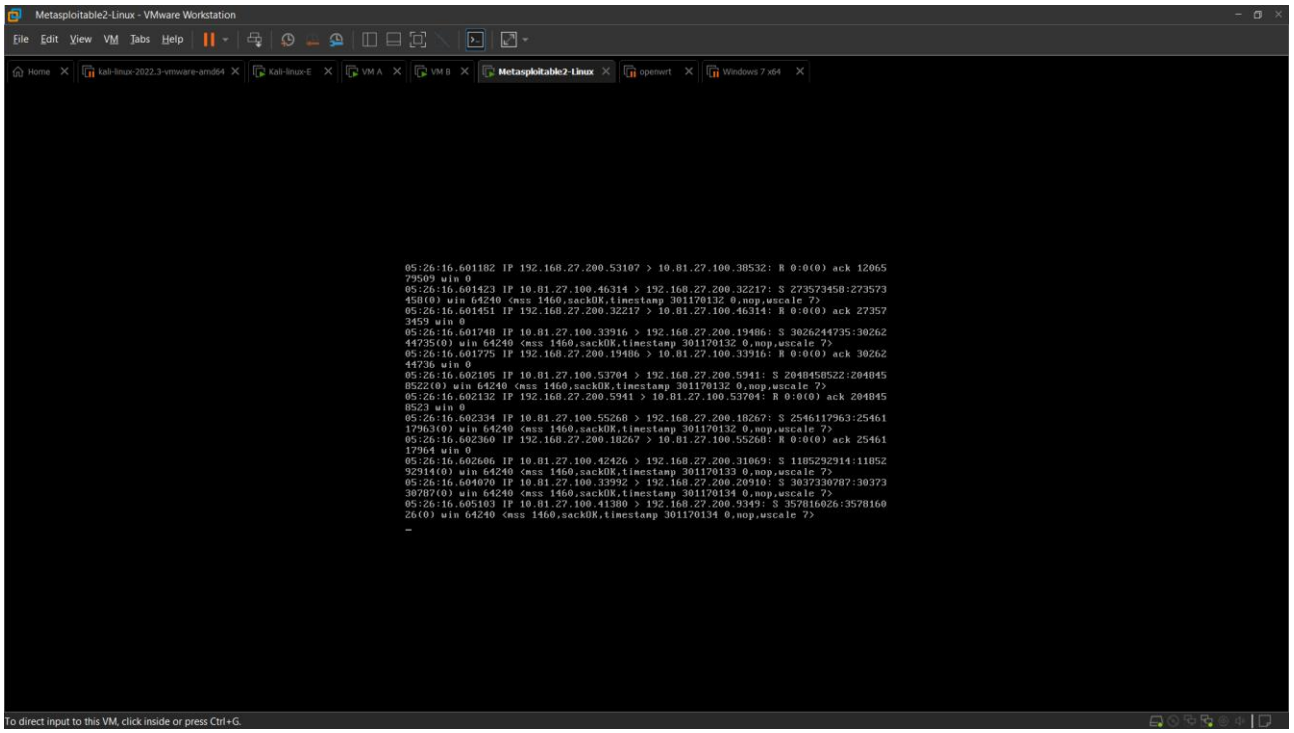


- Trước khi cài rules:

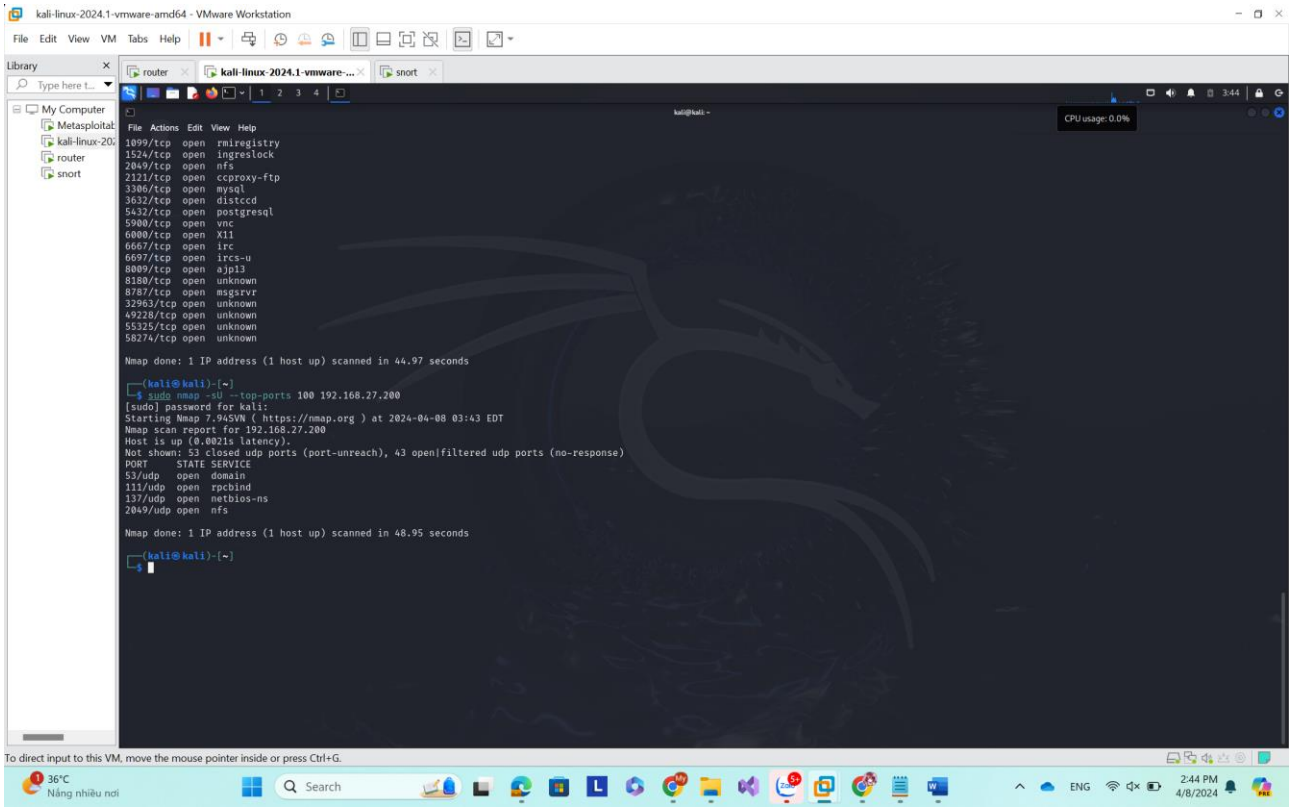
+ Kết quả scan các port và dịch vụ TCP:



+ Bên máy vintim nhận một loạt các gói khi thực hiện quét từ máy attacker:

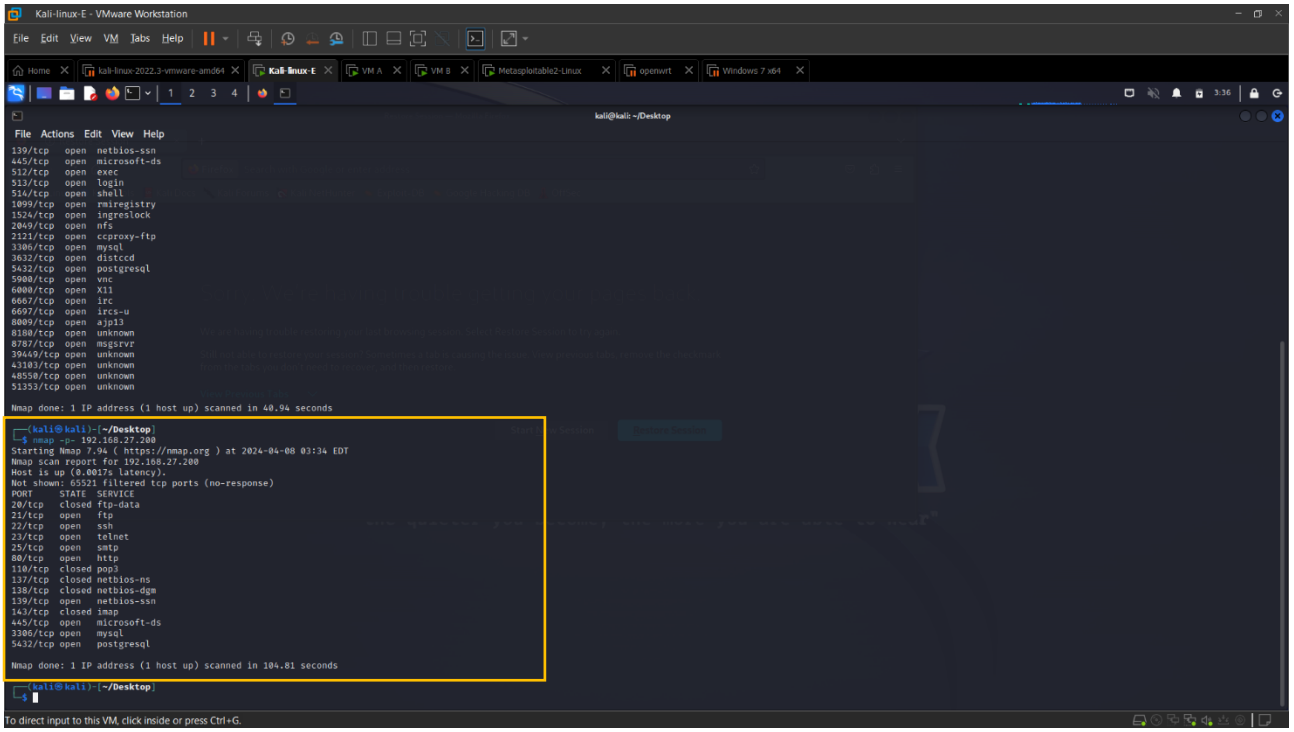


+ Kết quả scan các port và dịch vụ UDP:

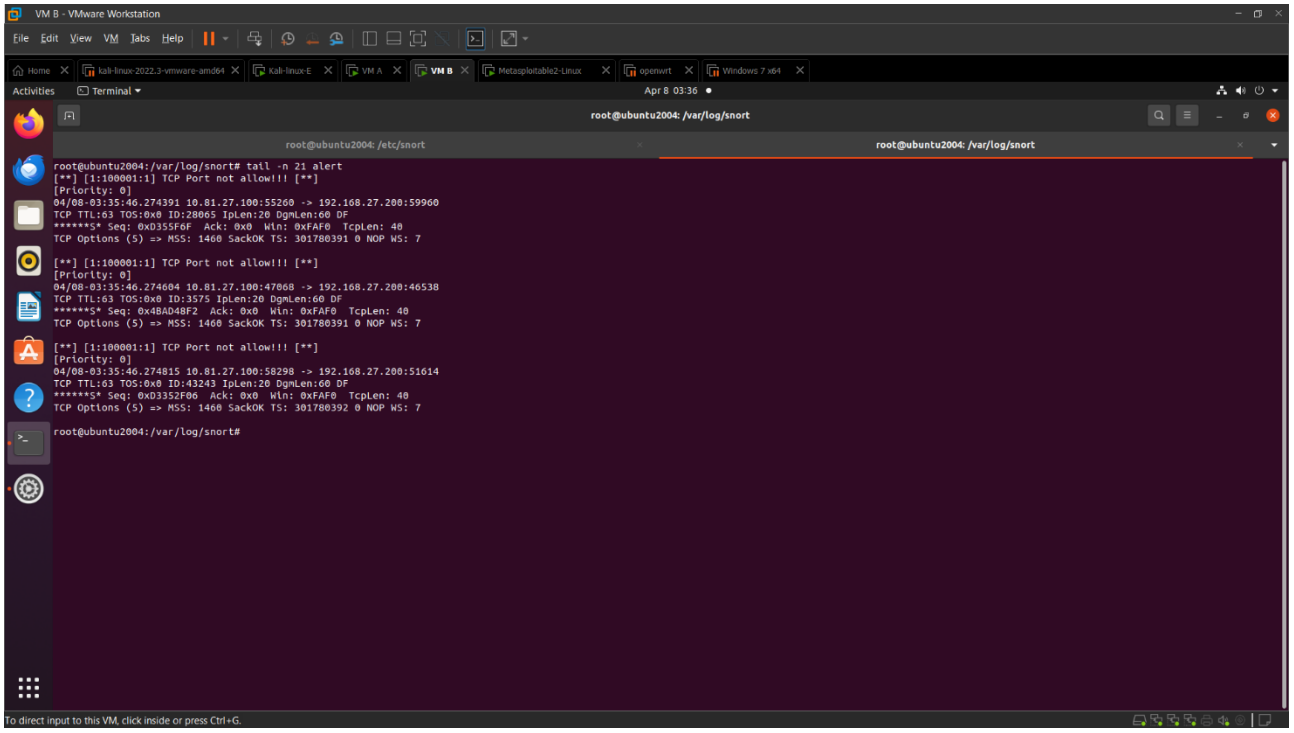


- Sau khi cài rules:

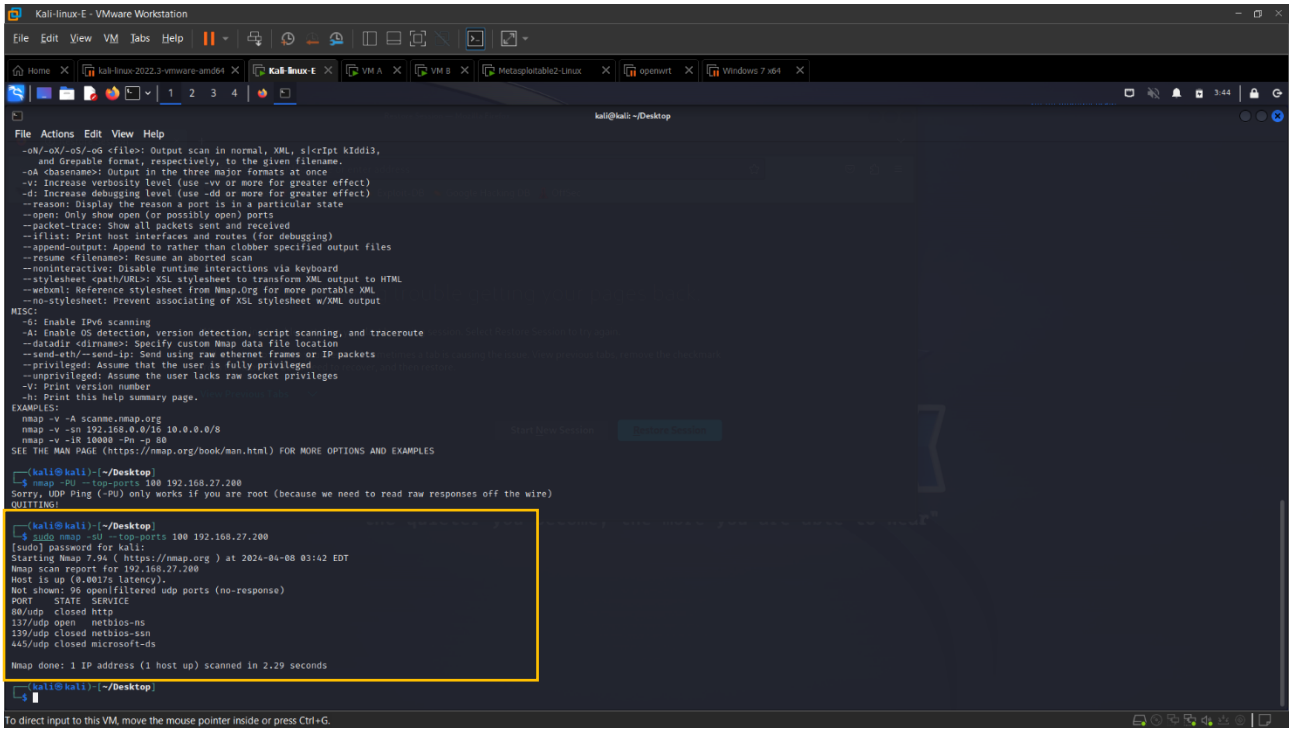
+ Kết quả scan các port và dịch vụ TCP: chỉ trả về các port liên quan đến các dịch vụ được phép truy cập, số lượng ít hơn so với trước khi áp dụng rules



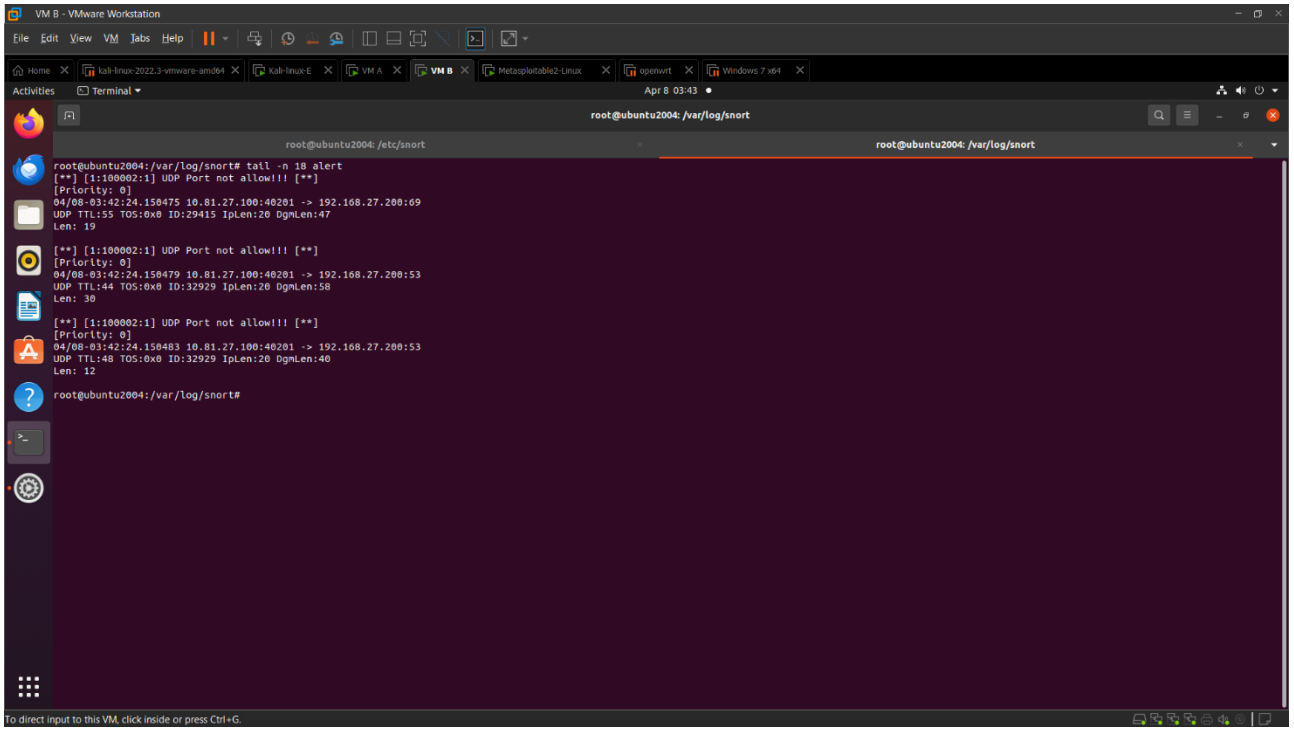
+ Trong log của snort ghi lại thông tin:



+ Kết quả scan các port và dịch vụ UDP: chỉ trả về các port liên quan đến các dịch vụ được phép truy cập, số lượng ít hơn so với trước khi áp dụng rules:

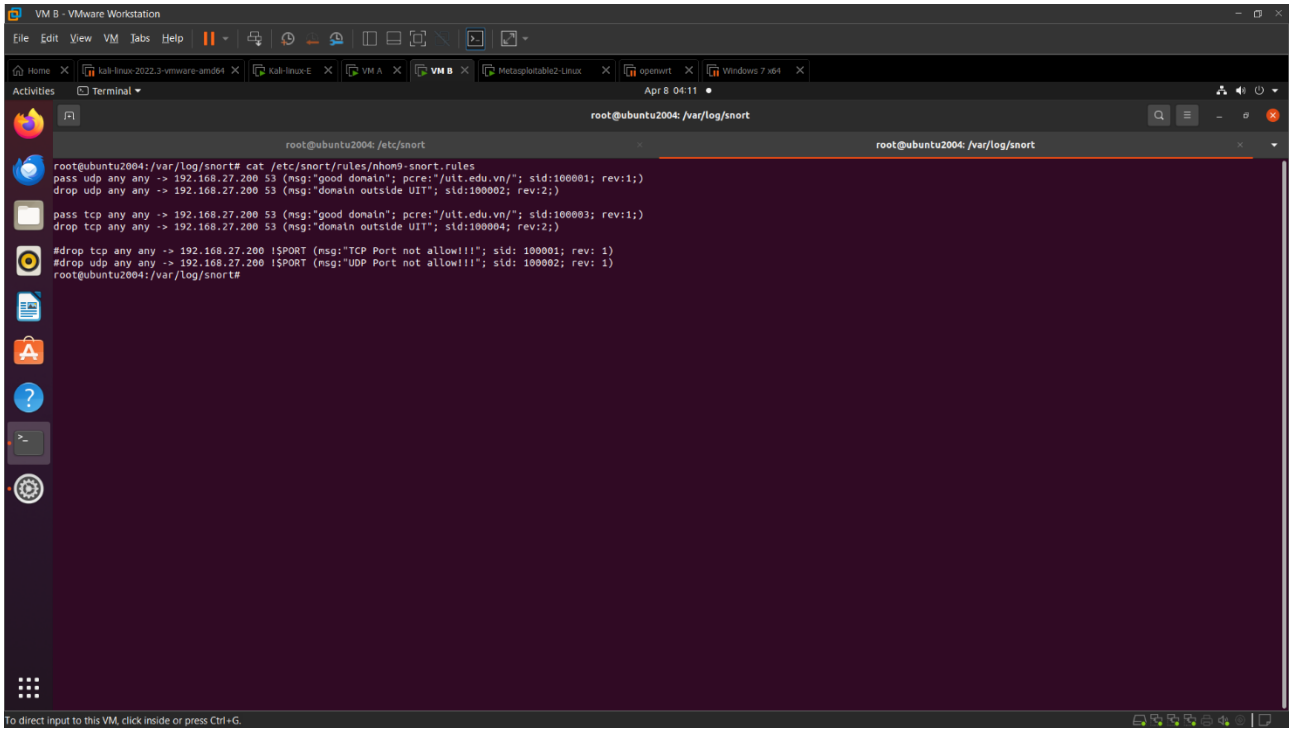


+ Trong log của snort ghi lại thông tin:

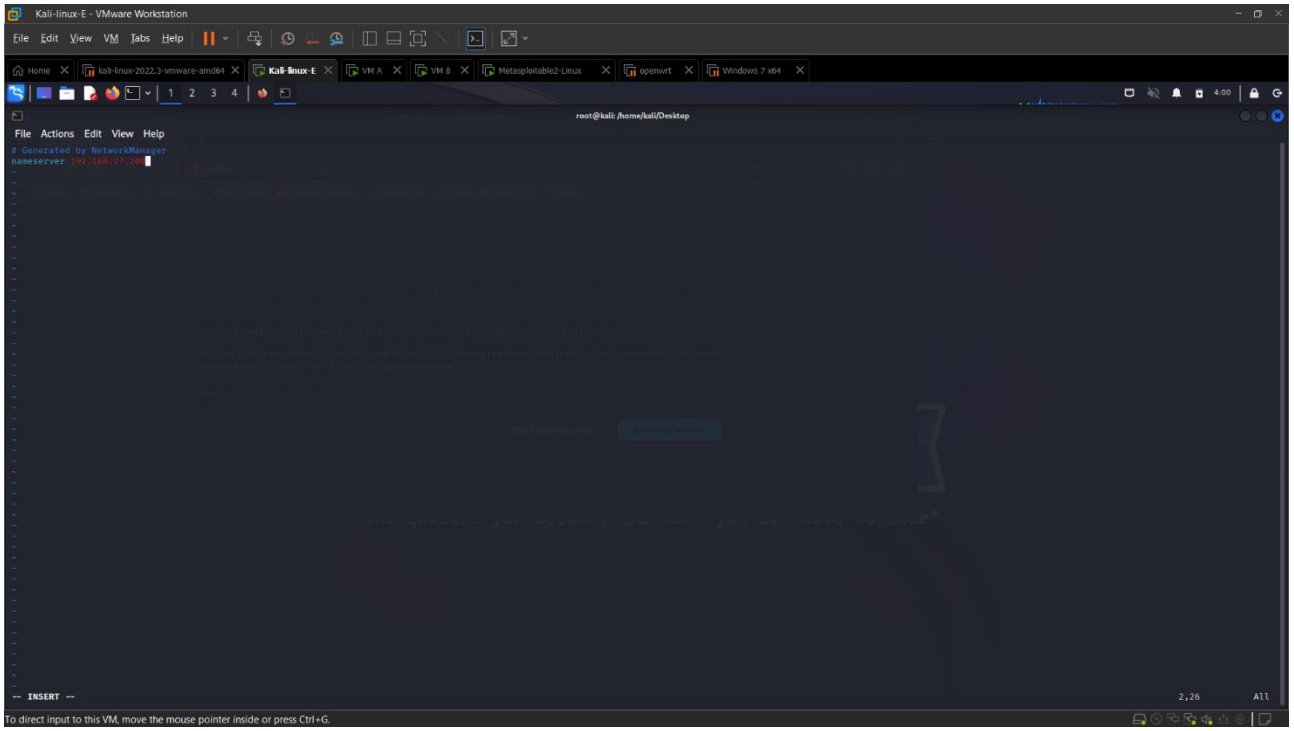


3. Yêu cầu 1.3: Chỉ cho phép truy vấn DNS đến các miền thuộc quản lý của UIT

- Snort rules:



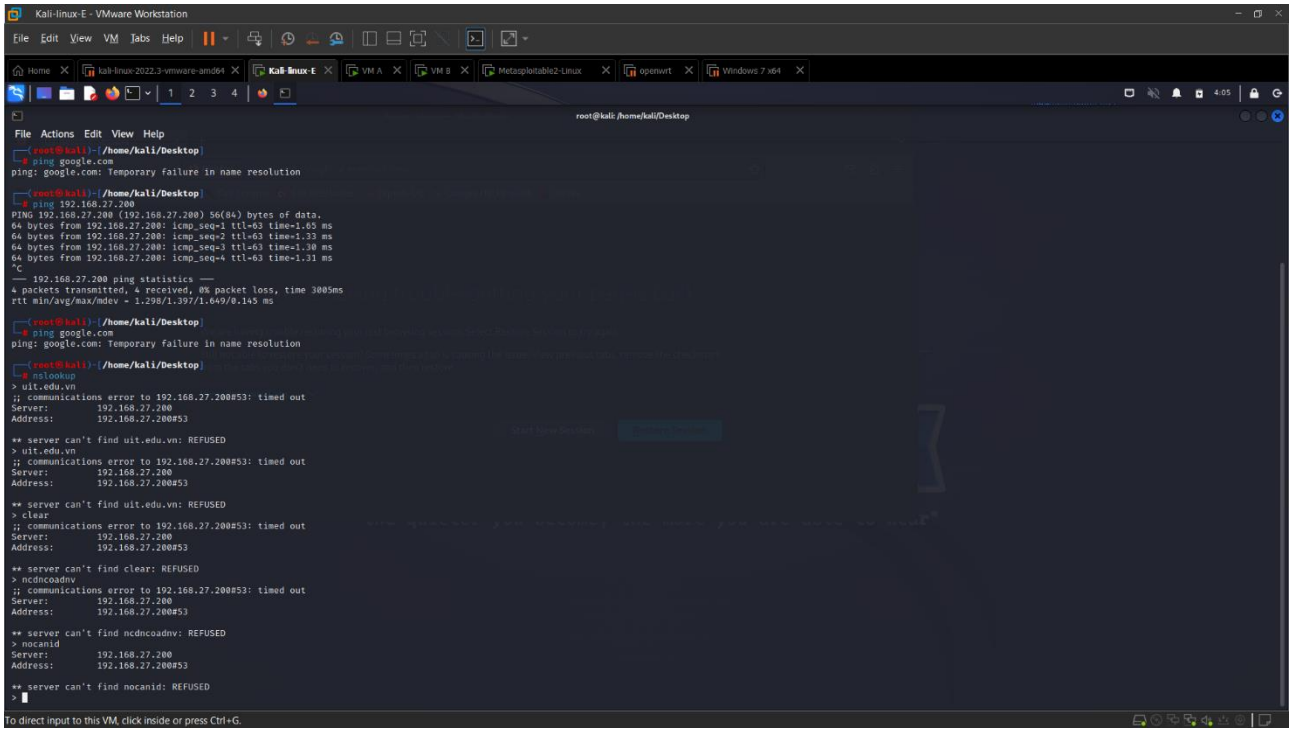
+ Ngoài ra, tiến hành chỉnh lại nameserver:



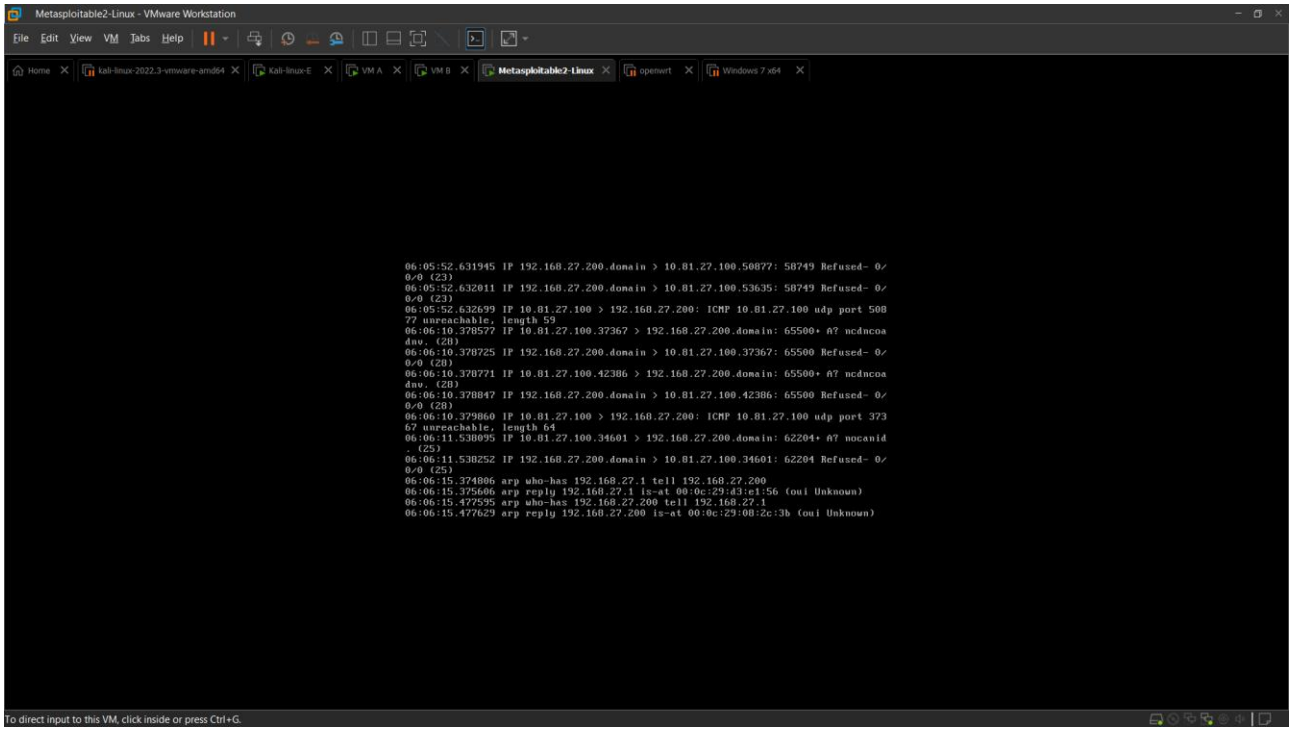
- Trước khi cài rules: Thực hiện nslookup luôn nhận được kết quả

Server: 192.168.27.200

Address: 192.168.27.200#53



+ Bên máy victim nhận và phản hồi refuse với mọi thực hiện nslookup

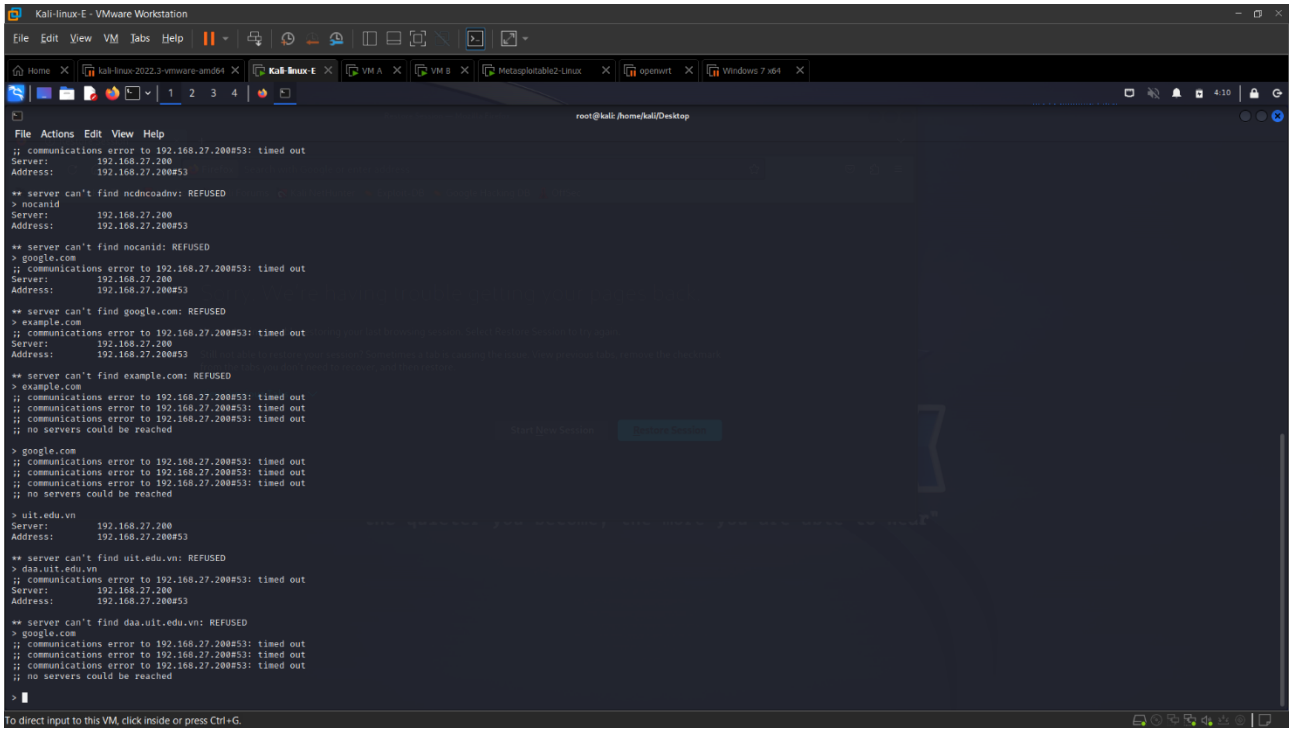


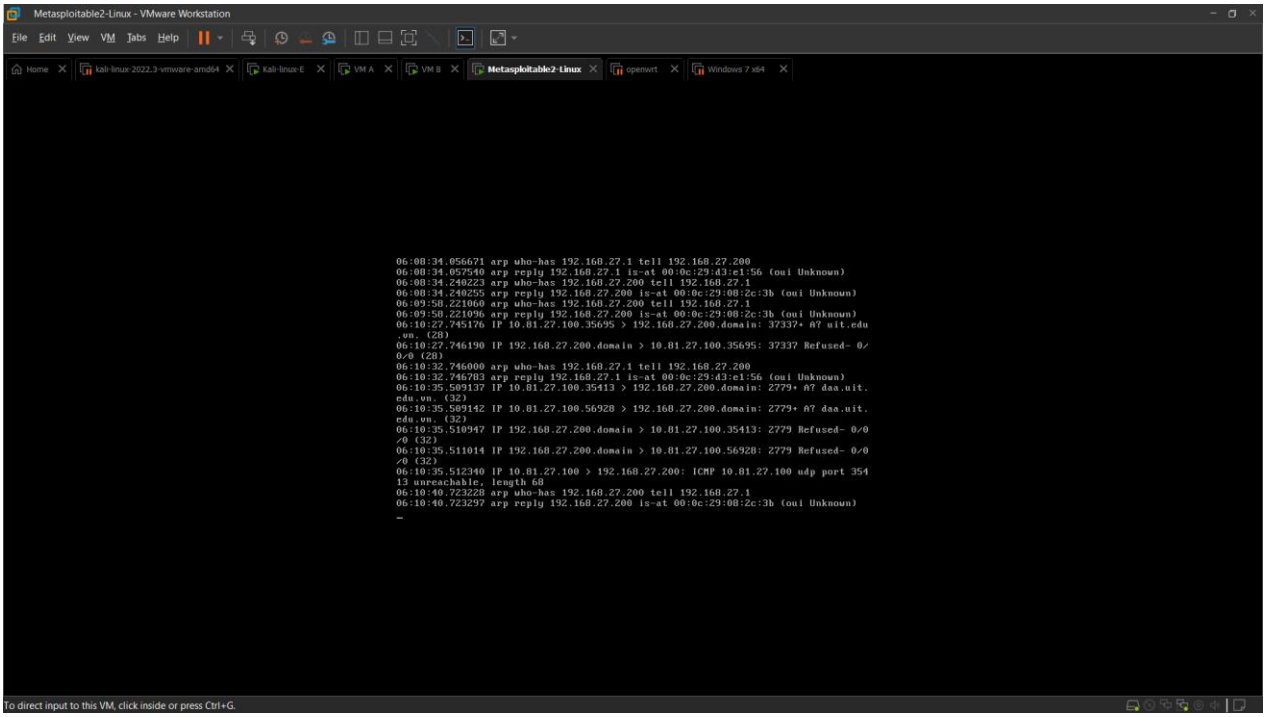
- Sau khi cài rules:

+ Chỉ khi thực hiện nslookup với các miền thuộc uit.edu.vn mới nhận được kết quả:

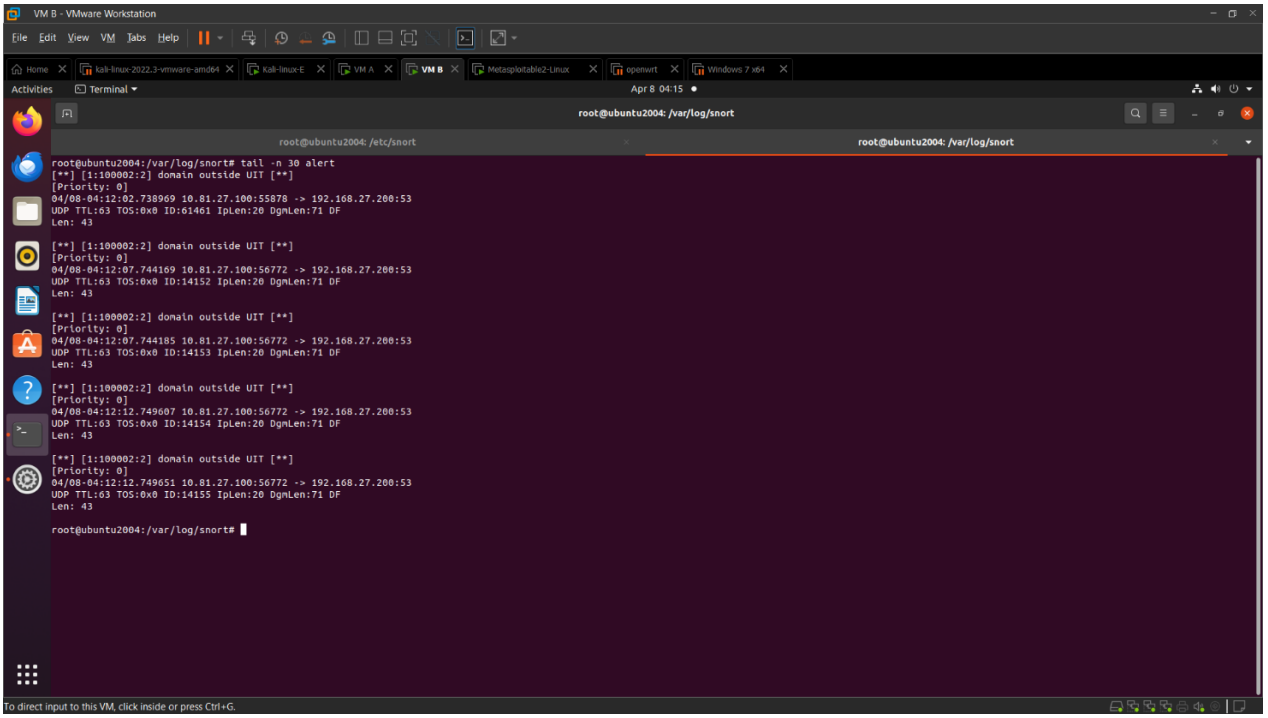
Server: 192.168.27.200

Address: 192.168.27.200#53





+ Trong log của snort ghi lại thông tin:



4. Yêu cầu 1.4: Ngăn chặn tấn công Time-based SQL Injection

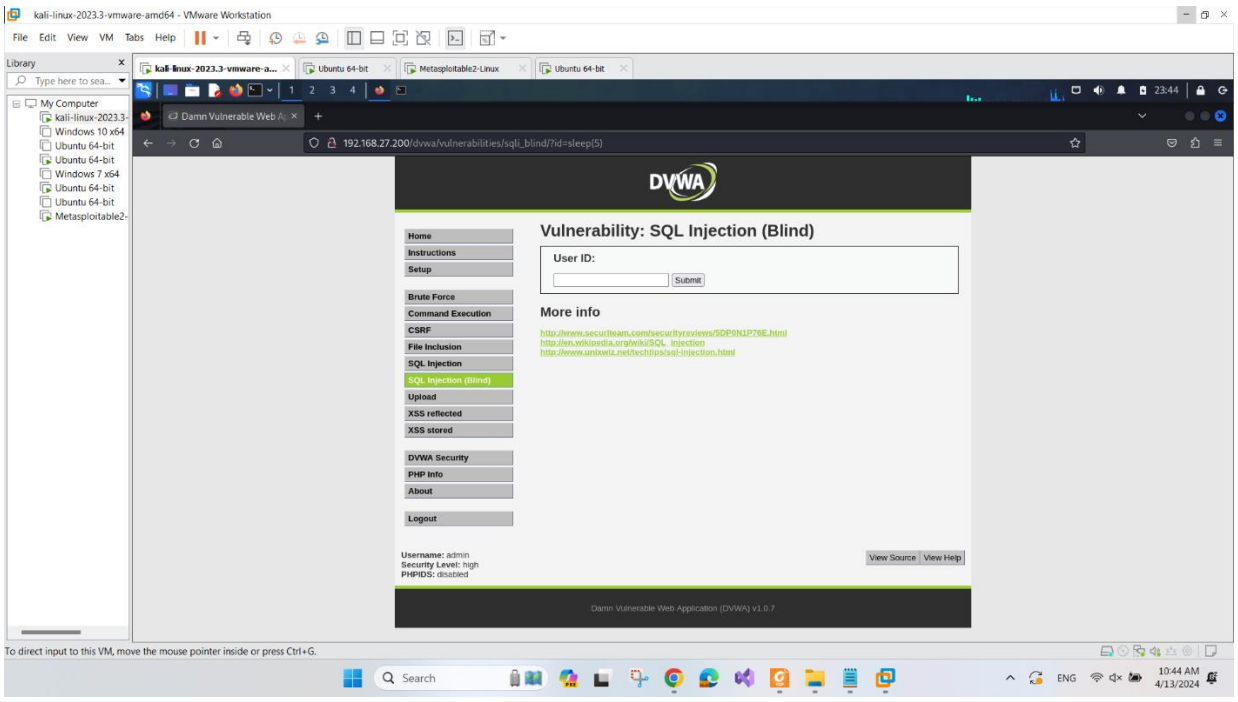
- Snort rules:

drop tcp any any -> any 80 (msg: "Time-based SQL Injection"; content: "sleep"; nocase; sid:1000005;)

drop tcp any any -> any 80 (msg: "Time-based SQL Injection"; content: "waitfor delay"; nocase; sid:1000006;)

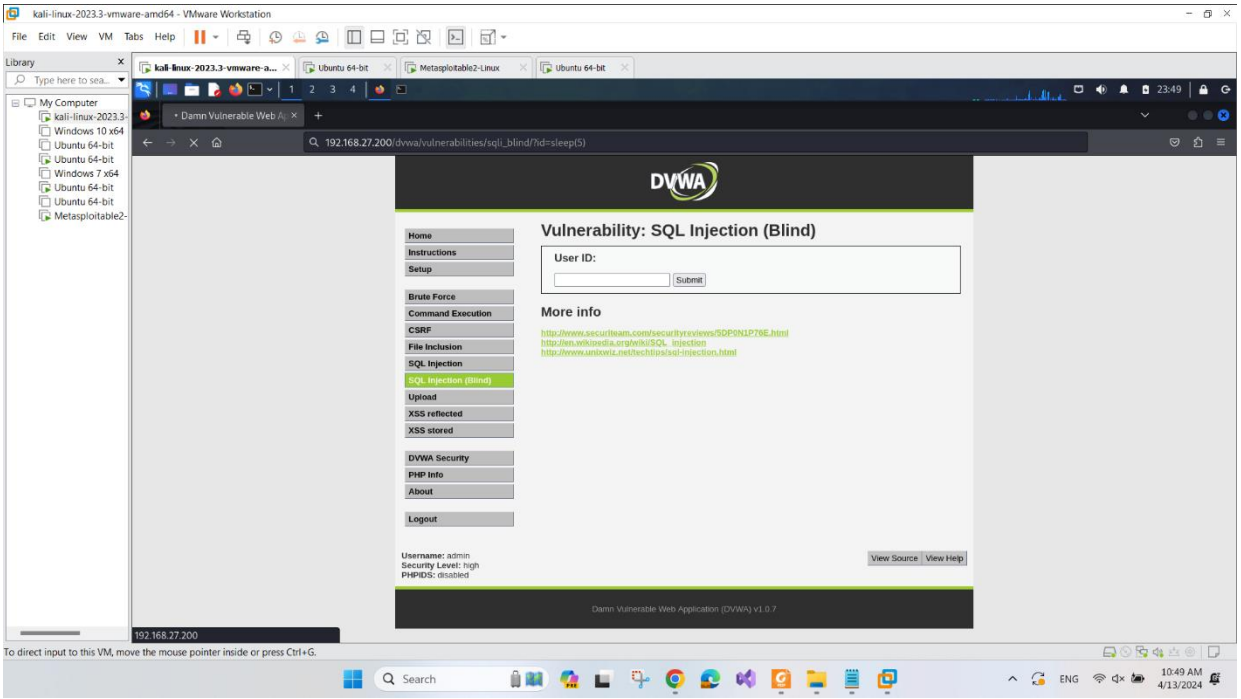
drop tcp any any -> any 80 (msg: "Time-based SQL Injection"; content: "benchmark"; nocase; sid:1000007;)

- Trước khi cài rules: Trang web truy cập bình thường và có thể thực hiện bindshell

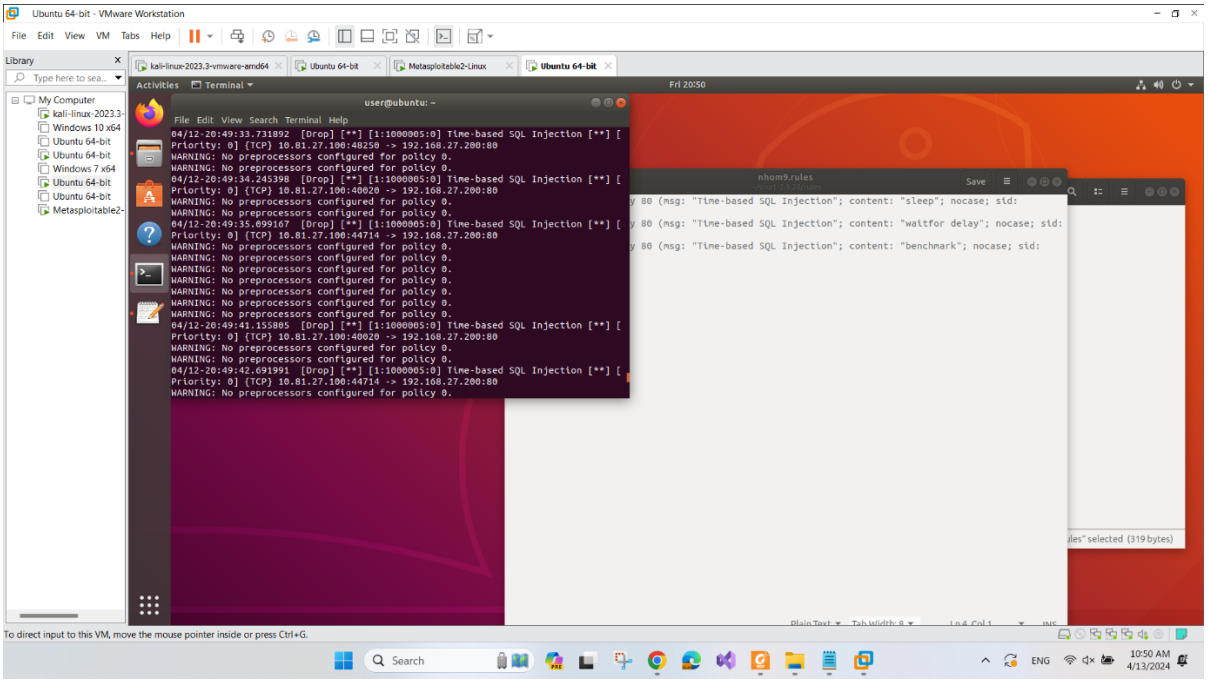


- Sau khi cài rules:

+ Tại trang web, web load trang mãi không vào được:



+ Tại snort, xuất hiện các dòng thông báo:



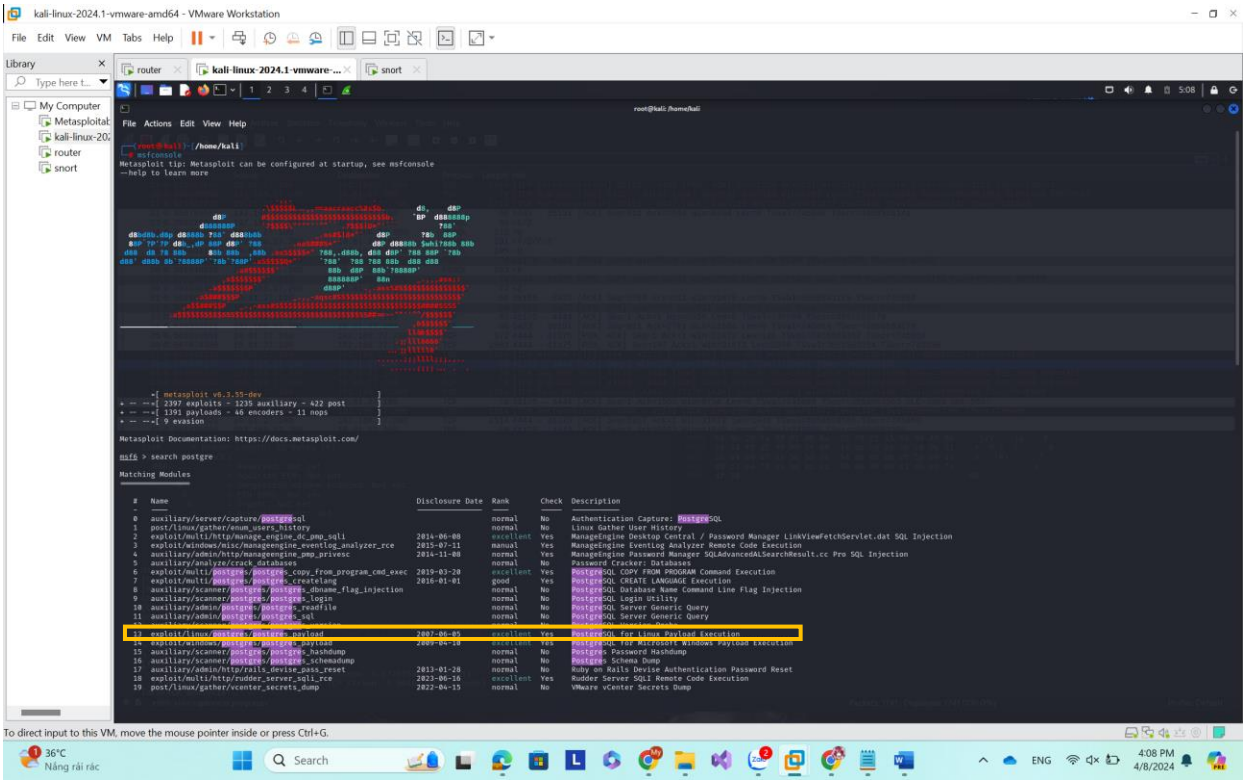
5. Yêu cầu 1.5: Sinh viên tự xây dựng thêm 2 kịch bản tấn công và viết Snort rule để ngăn chặn tấn công

a, Kịch bản 1: PostgreSQL for Linux Payload Execution

Trên một số bản cài đặt PostgreSQL mặc định của Linux, tài khoản dịch vụ postgres có thể ghi vào thư mục /tmp và cũng có thể lấy nguồn Thư viện chia sẻ UDF. Từ đó, cho phép thực thi mã tùy ý. Module này biên dịch một tệp đối tượng dùng chung của Linux, tải nó lên máy chủ đích thông qua phương pháp binary injection UPDATE pg_largeobject và tạo một UDF (user defined function) từ đối tượng dùng chung đó.

- Một số thông tin:

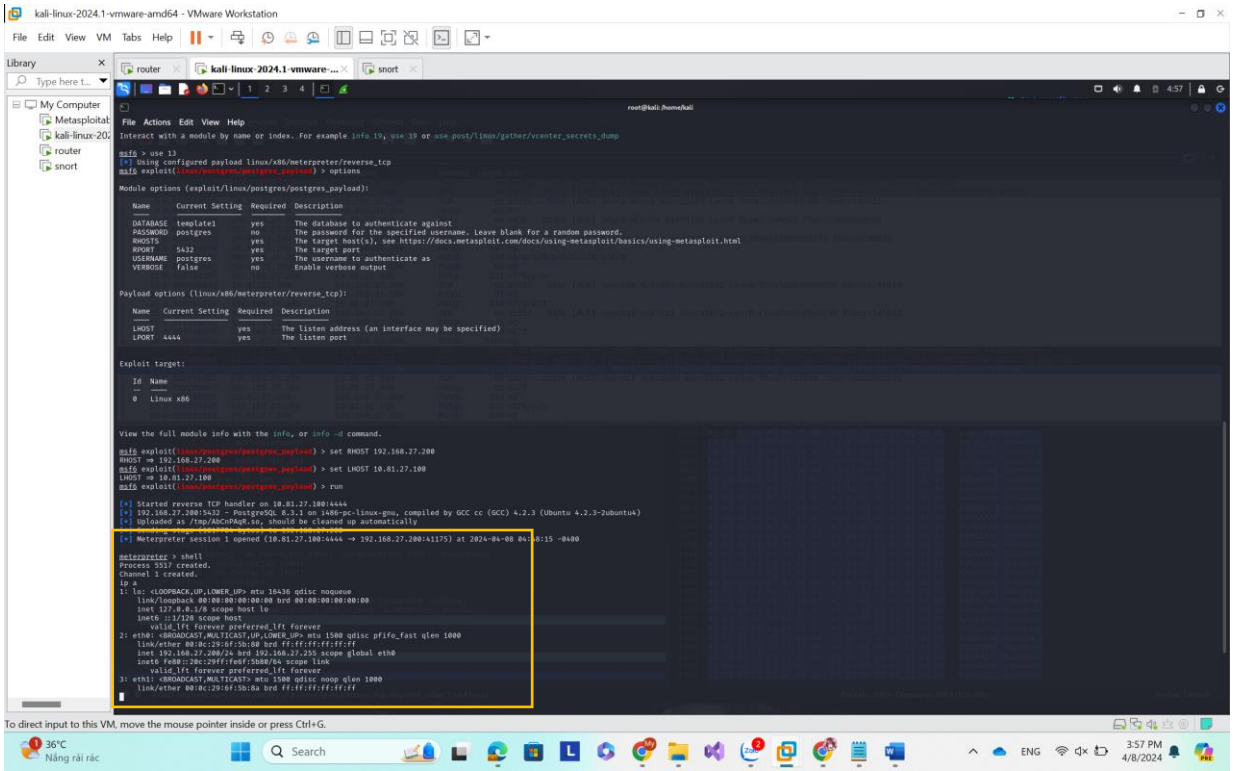
- **Name**: PostgreSQL for Linux Payload Execution
- **Module**: exploit/linux/postgres/postgres_payload
- **Source code:** modules/exploits/linux/postgres/postgres_payload.rb
- **Disclosure date**: 2007-06-05
- **Last modification time:** 2021-08-20 16:06:16 +0000
- **Supported platform(s):** Linux
- **Target service / protocol**: postgres
- **Target network port(s)**: 5432
- **List of CVEs**: CVE-2007-3280



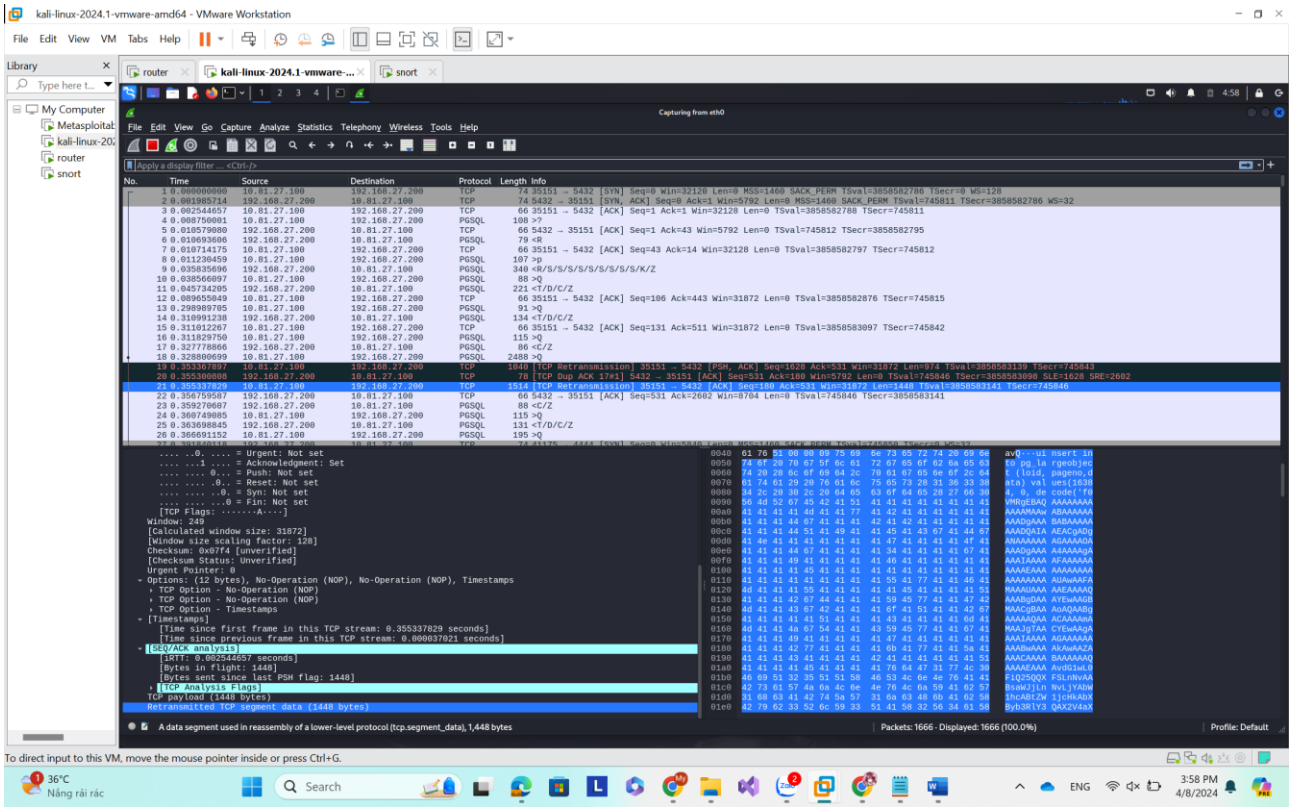
- Snort rules:

drop tcp any any -> 192.168.27.200 5432 (msg:"Detected PGSQL!"; content: "pg_largeobject"; sid:1000001; rev:1;)

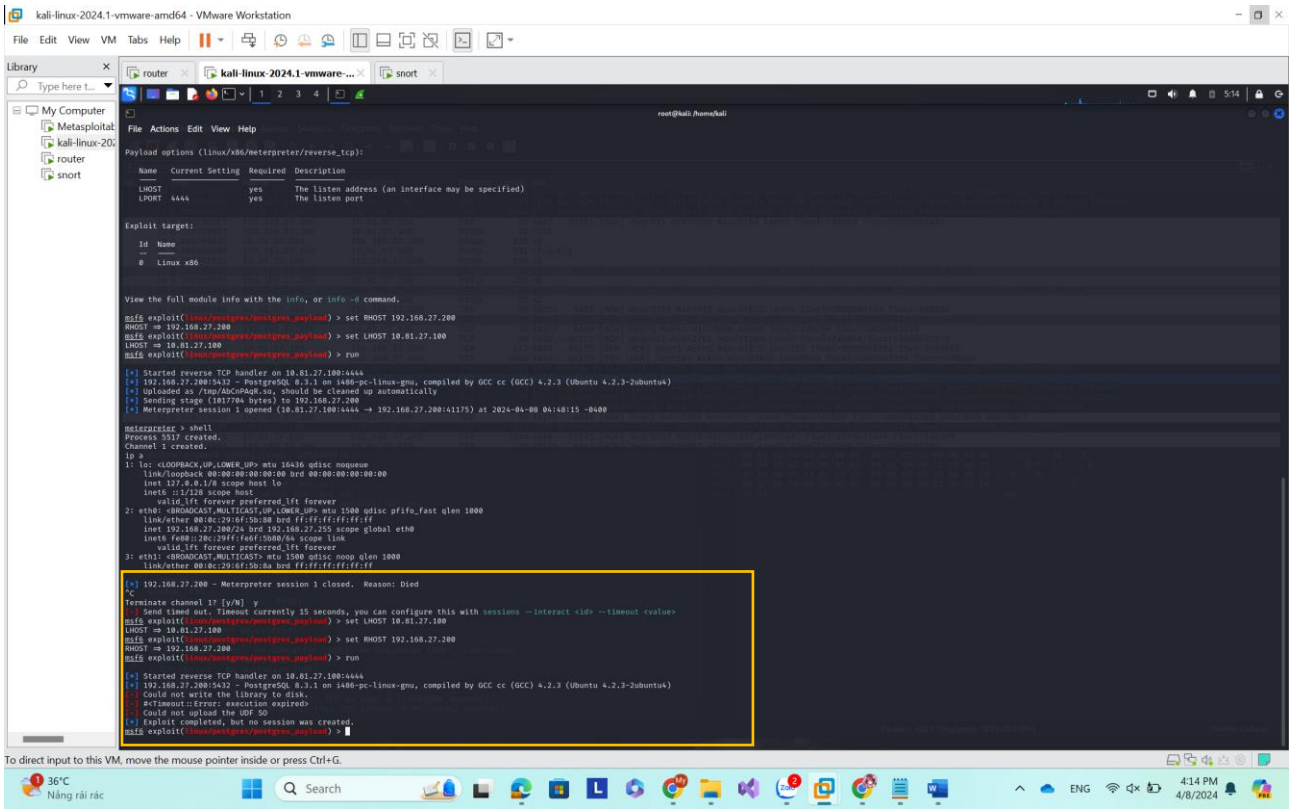
- Trước khi cài rules: Có thể tiến hành khai thác thành công



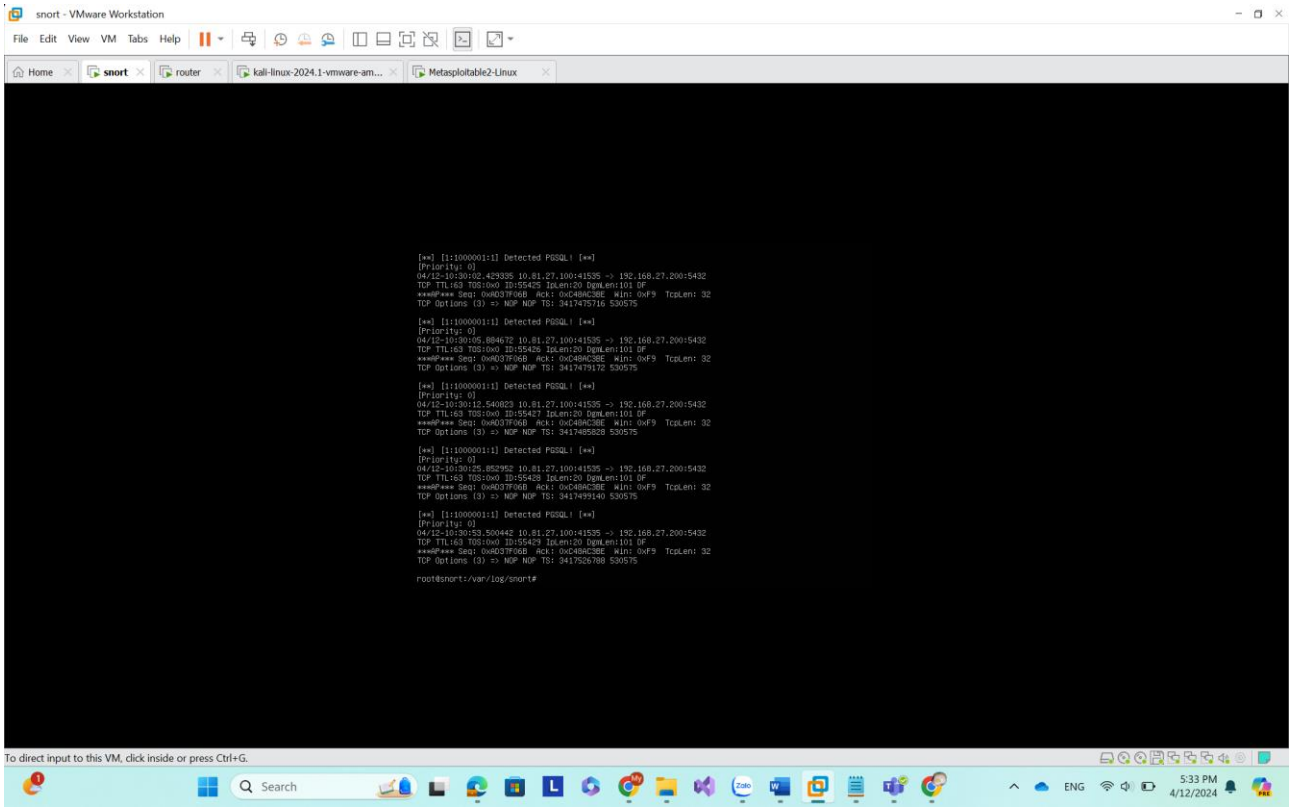
+ Dùng Wireshark bắt gói, nhận thấy có từ khoá pg_largeobject



- Sau khi cài rules: thất bại khi thực hiện tấn công



+ Tại snort, xuất hiện các dòng thông báo:



b, Kịch bản 2: VNC Authentication Scanner - Exploiting Port 5900 (VNC)

Virtual Network Computing (VNC) chạy trên cổng 5900, dịch vụ này có thể được khai thác bằng cách sử dụng một mô-đun trong Metasploit để tìm thông tin đăng nhập.

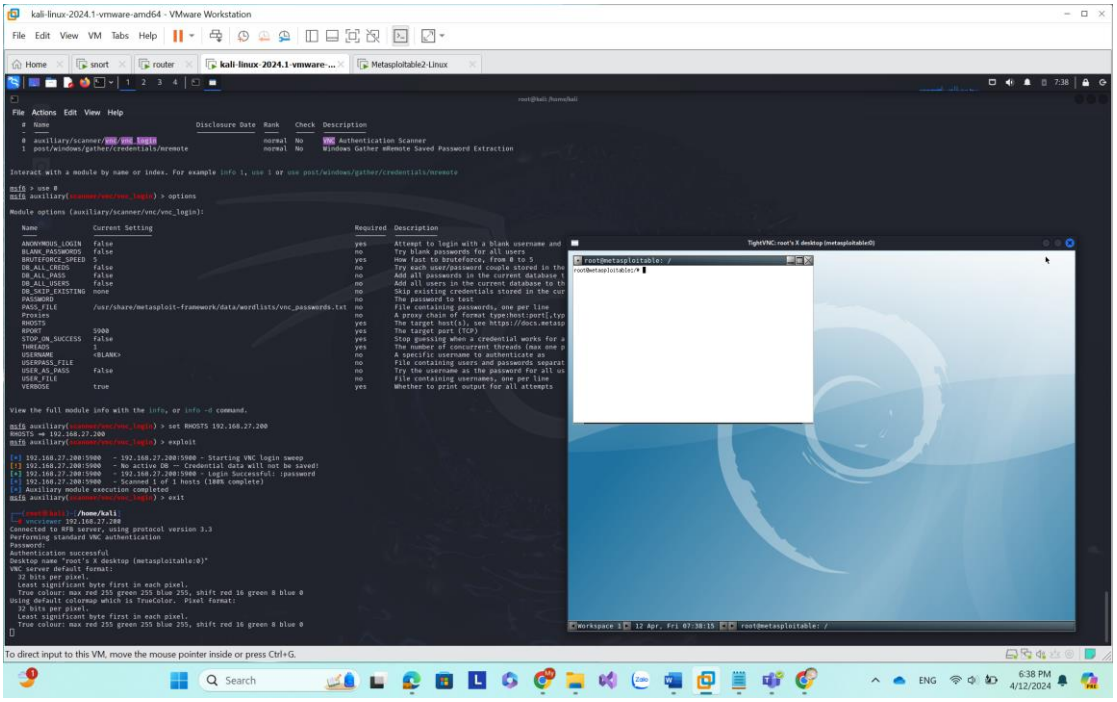
- Một số thông tin:

- **Name**: VNC Authentication Scanner
- **Module**: auxiliary/scanner/vnc/vnc_login
- **Source code:** modules/auxiliary/scanner/vnc/vnc_login.rb
- **Disclosure date**: -
- **Last modification time:** 2021-08-31 17:10:07 +0000
- **Supported platform(s):** -
- **Target service / protocol**: -
- **Target network port(s)**: 5900, 5901, 5902, 5903, 5904, 5905, 5906, 5907, 5908, 5909, 5910 (theo msfconsole, nó sử dụng port 5900 nên nhóm cũng sẽ trọng tâm ở port 5900).
- **List of CVEs**: CVE-1999-0506

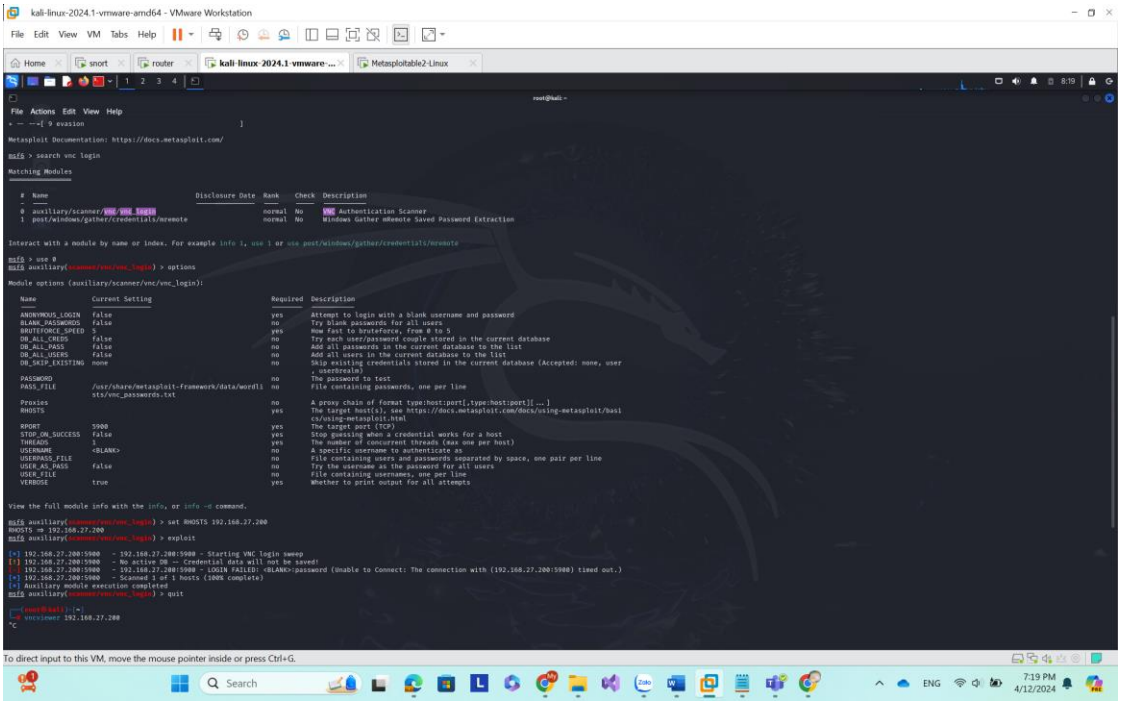
- Snort rules:

drop tcp any any -> 192.168.27.200 5900 (msg: "Detected VNC Login!"; sid:1000001; rev:1;)

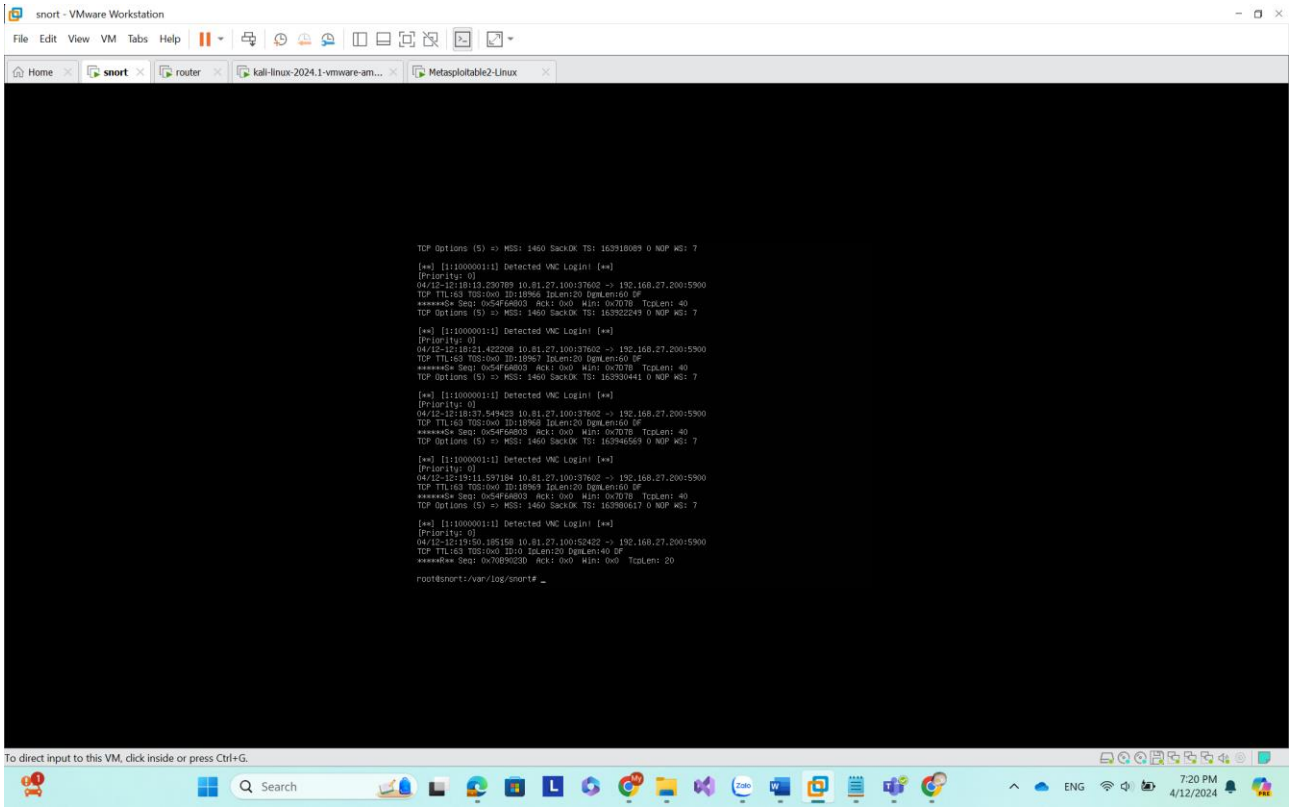
- Trước khi cài rules: nhận được “Login Successful”; đồng thời khi tiến hành mở vncviewer máy victim thành công



- Sau khi cài rules: nhận được “Login fail”; đồng thời khi tiến hành mở vncviewer máy victim không thành công



+ Tại snort, xuất hiện các dòng thông báo:



---HẾT---